EMR-ISAC
Emergency Management & Response-Information Sharing & Analysis Center

Highlights:

The U.S. Fire Administration maintains the **Emergency Management and Response – Information Sharing and Analysis Center (EMR-ISAC)**.

For information regarding the EMR-ISAC visit **www.usfa.dhs.gov/emr-isac** or contact the EMR-ISAC office at: **(301) 447-1325 and/or emr-isac@fema.dhs.gov.**

The InfoGram

Volume 15 – Issue 41 *October 8, 2015*

Intelligence Guide for First Responders

The Joint Counterterrorism Assessment Team (JCAT) has released the revised "Intelligence Guide for First Responders" (PDF, 24 Mb). Produced by first responders for first responders to encourage information sharing between all governmental agencies and levels, it is designed to assist public safety personnel in accessing and understanding intelligence reporting. The information in this guide was derived, compiled, and adapted from existing unclassified Intelligence Community and open-source information.

Federal, state, local, tribal, and territorial governments produce intelligence products every day that can be used by first responders. Learning first responders' roles and responsibilities as consumers of this information is a step in gaining access to this information. The guide also discusses how and why it must be protected, ways to access intelligence products, and what is required to gain access.

The guide is comprised of three sections:

- **How To** – discusses handling Sensitive But Unclassified information; gaining access to intelligence community information; understanding estimative language; and reporting suspicious activity with a nexus to terrorism.
- **General Information** – what intelligence is; what it can and cannot do; the intelligence cycle; categories of finished intelligence; the intelligence community; and intelligence products often available to first responders.
- **Reference** – terminology, acronyms, and abbreviations.

State, local, tribal, and territorial first responders and public safety professionals from around the country work side by side with federal intelligence analysts at the JCAT to research, produce, and disseminate counterterrorism intelligence. They offer fellowship opportunities to public safety professionals from state, local, tribal, and territorial government agencies such as law enforcement, emergency medical services, fire service, and public health officials.

(Source: JCAT)

Cybercrime Response Costs Plenty

2015 brought big stories in the field of cybersecurity, most notably the breaches of the government's Office of Personnel and Management (OPM). Several million current and former federal employees and contractors had a variety of personal informa-

tion and data stolen by the Chinese. The government is still working to react to this breach, and individuals are left to wonder how this may affect them long-term.

This large-scale incident is mirrored in small ways every day in private companies, state and local governments, and by individuals. Costs associated with cybercrimes are climbing. While Congress debates bills to handle this issue, the Emergency Services Sector (ESS) is not immune. Law enforcement agencies are seeing more ransomware attacks, PSAPs are vulnerable to a variety of attacks, and all first responder departments are targets of nuisance attacks.

Now is a good time to bolster your agency's cybercrime plan. This year, National Cyber Security Awareness Month has a page of resources for law enforcement and government agencies, and general tips anyone should make part of their personal safety and security routine.

(Source: DHS)

Emergency Plans Training for Rural Regions

The week of November 5th will see a focus on emergency planning for rural areas as the Center for Domestic Preparedness (CDP) teams up with the Rural Domestic Preparedness Consortium (RDPC).

Responders interested in this program will take the 8-hour Emergency Operations Plans for Rural Jurisdictions course to learn skills to develop an emergency operations plan for their local jurisdiction or region. They then have the choice to take either of these 3-day courses:

- Incident Command: Capabilities, Planning and Response Actions for All Hazards, a course that provides management-level responders with knowledge of how decisions made can impact the handling of a chemical, biological, radiological, nuclear, or explosive (CBRNE) incident, or
- Field Force Command and Planning, a course that prepares the student to serve as a member of an incident management team during a civil action or disorder.

All participants must register by Oct. 22, 2015, 5 p.m. to ensure their spot in the course. These will be held at the CDP in Anniston, Alabama. To register or to learn more about these and other training programs, please visit the CDP website. For assistance or more information, contact Mike Aguilar, the CDP Registrar, (256) 231-0106 or Michael.Aguilar@fema.dhs.gov.

(Source: CDP)

Comments Sought on FirstNet Cybersecurity

This week, FirstNet released the outline of its proposed cybersecurity plans and is requesting public comments and input no later than Friday, October 16th – a 2-week turnaround. Officials said they have received several requests for time extensions and are considering them.

Cybersecurity is a big concern for FirstNet as emergency communications have repeatedly been targets of cybercrime. The program has a rare opportunity to work cybersecurity policies into the design as they go rather than adding them into a finished network. FirstNet plans on releasing a final request for proposals by the end of 2015.

(Source: FirstNet)

DHS and the FBI encourage recipients of this document to report information concerning suspicious or criminal activity to the local *FBI office* and also the *State or Major Urban Area Fusion Center*.

For information specifically affecting the private sector critical infrastructure contact the **National Infrastructure Coordinating Center** by phone at **202-282-9201**, or by email at **nicc@dhs.gov**.